

Theory Problems:

1:

ECE 404 HW 4

1.) A.)
$$\begin{array}{r} 9x^5 + 4x^4 + 8x^3 + 2x^2 + 3x + 4 \\ 6x^5 + 2x^2 + 9x^3 + 7x^2 + 5x + 7 \\ \hline 15x^5 + 6x^4 + 17x^3 + 9x^2 + 8x + 11 \end{array}$$

$$(4x^5 + 6x^4 + 6x^3 + 9x^2 + 8x)$$

B.)
$$(8x^3 + 6x^2 + 8x + 1)(3x^3 + 9x^2 + 7x + 5)$$

$$(24x^6 + 72x^5 + 56x^4 + 40x^3) + (18x^5 + 54x^4 + 42x^3 + 30x^2) + (24x^4 + 72x^3 + 56x^2 + 40x) + (3x^3 + 9x^2 + 7x + 5)$$

$$24x^6 + 90x^5 + 134x^4 + 157x^3 + 95x^2 + 47x + 5$$

g.f.(ii)
$$\downarrow$$
 ~~24x^6 + 90x^5 + 134x^4 + 157x^3 + 95x^2 + 47x + 5~~

$$(2x^6 + 2x^5 + 2x^4 + 3x^3 + 7x^2 + 3x + 5)$$

C.)
$$\frac{3x^3 - 5x^2 + 10x - 3}{3x + 1}$$

g.f.(iii)
$$\downarrow$$

$$\begin{array}{r} 3x+1 \overline{) 3x^3 + 8x^2 + 10x - 3} \\ \underline{3x^3 + x^2} \\ 5x^2 + 10x - 3 \\ \underline{5x^2 + 9x} \\ x - 3 \end{array}$$

$$\rightarrow \boxed{x^2 + 9x + \frac{x-3}{3x+1}}$$

2:

ECE 404 HW 4
2.) A.) GF(2³) x^3+x+1

$$(x^2+x+1) \cdot (x^2+x)$$

$$\frac{x^4 + 2x^3 + 2x^2 + x}{x^3 + x + 1} = \frac{x^2 - 2x - 2}{x^3 + x + 1} + x + 2$$

$$\frac{x^4 + x}{x^3 + x + 1} = x - \frac{x^2}{x^3 + x + 1}$$

$$x^2 \rightarrow 100$$

B.) $(x^2) - (x^2 + x + 1)$

$$x + 1 \rightarrow 011$$

C.) $\frac{(x^2+x+1)}{x^2+1} \rightarrow \frac{(x^2+1)}{x^2+1} + \frac{x}{x^2+1}$

$$1 + \frac{x}{x^2+1} \rightarrow x \rightarrow 010$$

Programming Assignment:

In this we implement AES encryption utilizing its standard steps:

1. Byte substitution
2. Row Shifting
3. Mix Columns
4. Addition of the Round Keys

We create helper functions that we call in main to implement this process for encryptions